

Linux Network Servers

OpenVPN

Objetivos

Entender como funciona uma VPN
Configurar uma VPN host to host

O que é uma VPN?

VPN Virtual Private Network, é uma rede de comunicação particular, geralmente utilizando canais de comunicação inseguros, como a própria LAN ou mesmo a Internet. O que torna esta rede de comunicação particular é o fato das ferramentas de VPN empregarem métodos e protocolos de criptografia, criando um túnel de criptografia para prover acesso seguro a partes da rede ou mesmo ligação entre LAN's geograficamente separadas, eliminando a necessidade de um canal de comunicação privativo de alto custo fornecido pela operadora de telecomunicações.

Também podemos utilizar uma ferramenta de VPN para implementar ou reforçar a segurança de acesso há algum serviço dentro de nossa rede. Você possui um software de geração de notas fiscais, e os funcionários acessam este terminal via telnet, que é um protocolo que não implementa criptografia.

Para corrigir esta situação e reforçar a segurança deste ambiente, você poderia configurar uma VPN entre o computador dos usuários e o servidor, melhorando assim a segurança deste serviço.

Por que usar o OpenVPN?

- Simplicidade na configuração;
- Flexível;
- Muito seguro;
- Possui versões para Linux e Windows, é possível criar túneis entre duas máquinas usando esses sistemas;

Iremos configurar uma VPN host-to-host.

Nós trabalharemos neste laboratório com um par de chaves simétricas, ou seja, usaremos a mesma chave tanto para o servidor VPN quanto para o cliente VPN, logo, a chave deve ser gerada no servidor e replicada para o cliente via SSH.

Linux Network Servers

Configurando o servidor

O primeiro passo é instalar o software OpenVPN:

```
# aptitude install openvpn
```

Qual o módulo preciso levantar para usar o OpenVPN?

Módulo tun.

```
# modprobe tun
# echo "tun" >> /etc/modules
```

Cenário:

Ips do servidor:

IP remoto: 192.168.1.1 (isso só para testes em uma rede local, o normal é usar um endereço válido na internet)

IP (interface virtual da VPN): 10.0.0.1

Ips da máquina cliente:

IP remoto: 192.168.1.2 (isso só para testes em uma rede local, o normal é usar um endereço válido na internet)

IP (interface virtual da VPN): 10.0.0.2

Testando a conexão entre duas máquinas sem encriptação:

Faça na máquina cliente:

```
# openvpn --remote 192.168.1.1 --dev tun0 --ifconfig 10.0.0.2 10.0.0.1
```

Linux Network Servers

Faça na máquina servidora:

```
# openvpn --remote 192.168.1.2 --dev tun0 --ifconfig 10.0.0.1 10.0.0.2
```

Execute o comando ifconfig na máquina cliente e você verá:
inet end: 10.0.0.2
P-a-P: 10.0.0.1

Para testar a conectiva basta pingar a máquina servidora e vice-versa!

Agora vamos encriptar o túnel!
Vamos usar chaves estáticas. Um arquivo contendo o algoritmo de encriptação é usada por duas partes para encriptar os dados que serão transmitidos pela VPN.

Vamos entrar no diretório /etc/openvpn (no servidor) e gerar a chave:

```
# cd /etc/openvpn
# openvpn --genkey --secret /etc/openvpn/chave
```

Esse comando vai gerar um arquivo chamado "chave" em /etc/openvpn, que contém a chave de encriptação que será usada para criar a conexão.

"chave" é um arquivo de texto simples, que contém uma chave de 2048 bits.
Esse arquivo deverá ser copiado para o diretório /etc/openvpn do cliente.

É seguro enviar essa chave ao cliente por e-mail?

Não! O e-mail não é um meio seguro.

Quais alternativas então para enviar isso para a máquina cliente?

- sftp;
- scp;
- pendrive, hd externo etc;

Linux Network Servers

Acessar o arquivo "chave" no servidor:

```
# cd /etc/openvpn
# sftp root@192.168.1.1
Digite a senha!
sftp > cd /etc/openvpn
sftp > get chave
sftp > quit
```

Vamos gerar o arquivo de configuração do servidor:

```
# vim /etc/openvpn/server.conf

# Configuração para servidor
dev tun

# Server -> 10.0.0.1
# Client -> 10.0.0.2

# Definindo os IP's da VPN
ifconfig 10.0.0.1 10.0.0.2

# Definido a chave
secret /etc/openvpn/chave
# Definindo a porta
port 5000
comp-lzo
verb 4
```

Para que serve o parâmetro comp-lzo?

A função desse parâmetro é compactar dados transmitidos através do túnel.
O pacote "lzo" deve estar instalado.

Linux Network Servers

Configurando o cliente

Também é necessário ter o OpenVPN no cliente:

```
# aptitude install openvpn
```

Vamos gerar o arquivo de configuração do cliente:

```
# vim /etc/openvpn/client.conf

# Configuração para cliente
dev tun

# Server -> 10.0.0.1
# Client -> 10.0.0.2

# Definindo os IP's da VPN
ifconfig 10.0.0.2 10.0.0.1

# Definindo o IP real do servidor
remote 192.168.1.1

#Definido a chave
secret /etc/openvpn/chave

# Definindo a porta
port 5000
comp-lzo
verb 4
```

Iniciando a VPN, tanto no servidor quanto no cliente.

```
# openvpn --config /etc/openvpn/server.conf
# openvpn --config /etc/openvpn/client.conf
```

Linux Network Servers

Execute um ifconfig para ver se a interface tun0 foi criada:

```
# ifconfig -a
```

Execute um ping na sua interface VPN (servidor):

```
# ping 10.0.0.1
```

Execute um ping na interface do cliente:

```
# ping 10.0.0.2
```

Efetue testes em todos os serviços utilizando o IP da VPN.